ANUGRAH KIZHAKKE VEEDU

Kannur, Kerala, India | +91 8547743622 | anugrahkv07@gmail.com
linkedin.com/in/anugrah | github.com/Anugrahkv | Portfolio Website

PROFESSIONAL SUMMARY

Detail-oriented Cybersecurity professional and Master of Science (MSc) graduate uniquely positioned to bridge secure software engineering, systems administration, and network defense. Proficient in full-stack web development (Python, Django), REST API integrations, and deploying highly available Linux environments. Proven track record of architecting enterprise-grade IDS pipelines (pfSense, Suricata, ELK Stack) and automating Tier 1 SOC triage to reduce alert fatigue. Dedicated to leveraging practical engineering experience to build resilient defenses and execute comprehensive threat analysis mapped to the MITRE ATT&CK framework.

TECHNICAL SKILLS

Cybersecurity Operations: Incident Response, Threat Hunting, Log & Traffic Analysis, Packet Analysis (Wireshark), Vulnerability Assessments.
Security Architecture: Intrusion Detection Systems (Suricata), Next-Generation Firewalls (pfSense, FortiGate), SIEM (ELK Stack, Splunk), Network Segmentation, TCP/IP.
Systems Administration: Linux/Ubuntu Server, Infrastructure Provisioning, User Access Control, Server Hardening, System Backup & Disaster Recovery, Patch Management.
Secure Development & Automation: Python, Bash Scripting, Django, REST APIs, JSON Parsing, SQLite, Secure Authentication Workflows.
Frameworks & Compliance: OWASP Top 10, NIST Cybersecurity Framework (CSF), MITRE ATT&CK.

WORK EXPERIENCE

Btrac Solutions | Kerala, India **July 2022 – March 2023**
Web Application Development Intern (Secure Coding Focus)

- Supervised day-to-day operations, log consistency, and system patch levels across internal evaluation servers and **3** isolated client-facing production hosting nodes.
- Implemented Object-Relational Mapping (ORM) database integrations and safe authentication protocols to safeguard sensitive data integrity for **1,000+** relational records.
- Championed secure software development by conducting active code reviews, proactively identifying and mitigating **OWASP Top 10 vulnerabilities** prior to release cycles.
- Collaborated directly with software teams to deploy environment updates and install system security patches, tracking performance optimizations that reduced page load latencies by **15%**.

PROJECTS

SOC Automation & Enrichment Dashboard **June 2026**
Technologies: Python, Django, REST APIs (VirusTotal v3, AbuseIPDB), JSON

- Engineered a custom Tier 1 SOC triage dashboard utilizing Python and Django to automate the enrichment of Indicators of Compromise (IOCs) and reduce manual alert fatigue.
- Developed intelligent backend auto-routing logic and integrated RESTful APIs to extract and parse complex JSON threat intelligence for network reputation and multi-engine malware telemetry.
- Implemented strict environmental isolation and `.env` secret management to ensure API credentials remained securely excluded from version control.
- Conducted rigorous True Positive and True Negative validation simulations against live malware hashes (e.g., WannaCry) and active scanner IPs to verify engine accuracy.

Intrusion Detection & Threat Monitoring System (IDS) **September 2023 – September 2024**

Cybersecurity Graduate Researcher (Master's Project) | *Teesside University*

- Designed and deployed an integrated Intrusion Detection System (IDS) to actively monitor, detect, and isolate unauthorized network traffic anomalies across **10,000+** daily data streams.
- Configured a pfSense firewall interface and integrated Suricata IDS to establish real-time threat detection, engineering **15+ custom rules** that reduced false-positive alerts by **20%**.
- Deployed the ELK Stack to aggregate high-volume syslog data, constructing interactive Kibana dashboards that reduced issue resolution time by **30%**.
- Transformed raw, noisy system data into a clean, monitored baseline to ensure infrastructure resilience and high availability.

TrippyGo – Secure Full-Stack Web Application **2023**

Technologies: Python, Django, HTML, CSS, SQLite

- Developed a scalable travel management application from scratch, prioritizing modern data protection standards to safely process **500+** simulated user query interactions.
- Implemented robust authentication workflows, cryptographic session management, and strict form validation to systematically eliminate **100%** of SQL Injection (SQLi) and Cross-Site Scripting (XSS) vulnerabilities.
- Applied MVC architecture principles and developed scheduled maintenance scripts to guarantee secure database handling with **zero deployment downtime** in simulated production environments.

CERTIFICATIONS & TRAINING

Certified IT Infrastructure & Cyber SOC Analyst (CICSA) **Expected October 2026**

Certified Ethical Hacker (CEH) **Expected October 2026**

Linux Fundamentals | *Hack The Box Academy* **June 2026**

Fortinet Certified Associate (FCA) in Cybersecurity **June 2026**

Fortinet | Validation ID: 9668149803AK

Fortinet Certified Fundamentals (FCF) in Cybersecurity **June 2026**

Fortinet | Validation ID: 7103587775AK

EDUCATION

Teesside University | Middlesbrough, UK **2023 – 2024**

Master of Science in Cyber Security

Kannur University | Kerala, India **2020 – 2023**

Bachelor's Degree in Computer Application